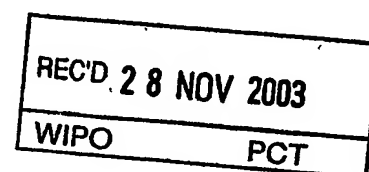




# BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE



Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 13 NOV 2003

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS  
CONFORMÉMENT À LA  
RÈGLE 17.1.a) OU b)

Martine PLANCHE

INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

SIEGE  
26 bis, rue de Saint Petersburg  
75800 PARIS cedex 08  
Téléphone : 33 (0)1 53 04 53 04  
Télécopie : 33 (0)1 53 04 45 23  
www.inpi.fr



Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W / 260899

REMISE DES PIÈCES

DATE 26 JUIL 2002

LIEU 54 INPI NANCY

N° D'ENREGISTREMENT

0209475

NATIONAL ATTRIBUÉ PAR L'INPI

DATE DE DÉPÔT ATTRIBUÉE

PAR L'INPI

26 JUIL. 2002

Vos références pour ce dossier

(facultatif) 016596

**1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE**  
À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BALLOT  
9 rue Claude Chappe  
Technopôle Metz 2000  
57070 METZ

Confirmation d'un dépôt par télécopie

☐ N° attribué par l'INPI à la télécopie

**2 NATURE DE LA DEMANDE**

Cochez l'une des 4 cases suivantes

Demande de brevet

☒

Demande de certificat d'utilité

☐

Demande divisionnaire

☐

*Demande de brevet initiale*

N°

Date / /

*ou demande de certificat d'utilité initiale*

N°

Date / /

Transformation d'une demande de

brevet européen *Demande de brevet initiale*

☐

N°

Date / /

**3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)**

Procédé de chiffrement de données, système cryptographique et composant associés.

**4 DÉCLARATION DE PRIORITÉ**

OU REQUÊTE DU BÉNÉFICE DE

LA DATE DE DÉPÔT D'UNE

DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation

Date / /

N°

Pays ou organisation

Date / /

N°

Pays ou organisation

Date / /

N°

☐ S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»

**5 DEMANDEUR**

☐ S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»

Nom ou dénomination sociale

GEMPLUS

Prénoms

Forme juridique

Société Anonyme

N° SIREN

Code APE-NAF

Adresse

Rue

Avenue du Pic de Bertagne  
Parc d'Activités de GEMENOS

Code postal et ville

13420 GEMENOS

Pays

FRANCE

Nationalité

Française

N° de téléphone (facultatif)

N° de télécopie (facultatif)

Adresse électronique (facultatif)





26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

REÇU LE BREVET D'INVENTION

29 IIII. 2002

CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



N° 11354\*01

BALLOT  
METZ

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W / 260899


<b>REMISE DES PIÈCES</b> DATE <b>26 JUIL 2002</b> LIEU <b>54 INPI NANCY</b>		<b>1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE</b> À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE  CABINET BALLOT 9 rue Claude Chappe Technopôle Metz 2000 57070 METZ	
N° D'ENREGISTREMENT <b>0209475</b> NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI			
Vos références pour ce dossier (facultatif) 016596			
Confirmation d'un dépôt par télécopie <input type="checkbox"/> N° attribué par l'INPI à la télécopie			
<b>2 NATURE DE LA DEMANDE</b>		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
Demande de brevet initiale		N°	Date
ou demande de certificat d'utilité initiale		N°	Date
Transformation d'une demande de brevet européen		<input type="checkbox"/>	Date
Demande de brevet initiale		N°	Date
<b>3 TITRE DE L'INVENTION</b> (200 caractères ou espaces maximum) Procédé de chiffrement de données, système cryptographique et composant associés.			
<b>4 DÉCLARATION DE PRIORITÉ</b> OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation Date N° Pays ou organisation Date N° Pays ou organisation Date N° <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
<b>5 DEMANDEUR</b>		<input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»	
Nom ou dénomination sociale		GEMPLUS	
Prénoms			
Forme juridique		Société Anonyme	
N° SIREN			
Code APE-NAF			
Adresse	Rue	Avenue du Pic de Bertagne Parc d'Activités de GEMENOS	
	Code postal et ville	13420	GEMENOS
Pays		FRANCE	
Nationalité		Française	
N° de téléphone (facultatif)			
N° de télécopie (facultatif)			
Adresse électronique (facultatif)			





REMISE DES PIÈCES DATE <b>26 JUIL 2002</b> LIEU <b>54 INPI NANCY</b> N° D'ENREGISTREMENT <b>0209475</b> NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI	
<b>Vos références pour ce dossier : (facultatif)</b>		016596	
<b>6 MANDATAIRE</b>			
Nom		LECLAIRE	
Prénom		Jean-Louis	
Cabinet ou Société		CABINET BALLOT	
N° de pouvoir permanent et/ou de lien contractuel			
Adresse	Rue	9 rue Claude Chappe - Technopôle Metz 2000	
	Code postal et ville	57070	METZ
N° de téléphone (facultatif)		03 87 74 81 36	
N° de télécopie (facultatif)		03 87 36 26 76	
Adresse électronique (facultatif)			
<b>7 INVENTEUR (S)</b>			
Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée	
<b>8 RAPPORT DE RECHERCHE</b>		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paiement échelonné de la redevance		Paiement en trois versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non	
<b>9 RÉDUCTION DU TAUX DES REDEVANCES</b>		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Requête antérieurement à ce dépôt (joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence):	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes			
<b>10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE</b> (Nom et qualité du signataire) LECLAIRE Jean-Louis 93.4009		<b>VISA DE LA PRÉFECTURE OU DE L'INPI</b>  Magali ROUX	



REMISE DES PIÈCES DATE <b>26 JUIL 2002</b> LIEU <b>54 INPI NANCY</b>		Réservé à l'INPI	
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI		<b>0209475</b>	
Vos références pour ce dossier : <i>(facultatif)</i>		<b>016596</b>	
<input checked="" type="checkbox"/> <b>MANDATAIRE</b>			
Nom		<b>LECLAIRE</b>	
Prénom		<b>Jean-Louis</b>	
Cabinet ou Société		<b>CABINET BALLOT</b>	
N° de pouvoir permanent et/ou de lien contractuel			
Adresse	Rue	<b>9 rue Claude Chappe - Technopôle Metz 2000</b>	
	Code postal et ville	<b>57070</b>	<b>METZ</b>
N° de téléphone <i>(facultatif)</i>		<b>03 87 74 81 36</b>	
N° de télécopie <i>(facultatif)</i>		<b>03 87 36 26 76</b>	
Adresse électronique <i>(facultatif)</i>			
<input checked="" type="checkbox"/> <b>INVENTEUR (S)</b>			
Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée	
<input checked="" type="checkbox"/> <b>RAPPORT DE RECHERCHE</b>		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paiement échelonné de la redevance		Paiement en trois versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non	
<input checked="" type="checkbox"/> <b>RÉDUCTION DU TAUX DES REDEVANCES</b>		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention <i>(joindre un avis de non-imposition)</i> <input type="checkbox"/> Requête antérieurement à ce dépôt <i>(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :</i>	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes			
<input checked="" type="checkbox"/> <b>SIGNATURE DU DEMANDEUR OU DU MANDATAIRE</b> (Nom et qualité du signataire) <b>LECLAIRE Jean-Louis 93.4009</b>		<b>VISA DE LA PRÉFECTURE OU DE L'INPI</b>  <b>Magali ROUX</b>	



PROCEDE DE CHIFFREMENT DE DONNEES, SYSTEME  
CRYPTOGRAPHIQUE ET COMPOSANT ASSOCIES

L'invention concerne un procédé de chiffrement, et un système cryptographique associé, avec application notamment dans le domaine de la cryptographie à clé publique. L'invention peut être mise en œuvre dans des dispositifs électroniques tels que des cartes à puce.

Un système cryptographique à clé publique complet comprend généralement un algorithme de chiffrement et un algorithme de signature. Un tel système cryptographique peut être mis en œuvre par exemple dans une carte à puce comprenant notamment, dans un circuit intégré, des moyens de calcul programmés pour mettre en œuvre les algorithmes, et des moyens de mémorisation, pour mémoriser des clés publiques et / ou des clés secrètes nécessaires à la mise en œuvre des algorithmes.

Un algorithme connu et utilisé dans les systèmes cryptographiques à clé publique est l'algorithme RSA (de Rivest, Shamir et Adleman). Il peut être utilisé pour réaliser des opérations de chiffrement et des opérations de signature. De manière général, l'algorithme RSA consiste à réaliser une opération d'exponentiation, à l'aide d'une clé publique ou privée, d'un message clair formaté par une fonction de formatage pour le chiffrement ou une fonction de formatage pour la signature, selon le cas.

Un procédé de chiffrement utilisant l'algorithme RSA consiste ainsi à formater un message clair  $m$  par une fonction  $\mu$  de formatage pour le chiffrement, puis à réaliser une exponentiation du résultat selon la relation :

$$c = f(\mu(m)) = [\mu(m)]^e \bmod N$$



où  $\mu$  est une fonction de formatage pour le chiffrement,  $(N, e)$  une clé publique, et  $f(x, N, e)$  la fonction d'exponentiation  $f(x, N, e) = x^e \bmod N$ .

Le message chiffré  $c$  peut ensuite être déchiffré en utilisant à nouveau l'algorithme RSA, avec la fonction inverse  $f^{-1}(x, N, d)$ ,  $(N, d)$  étant une clé privée associée à la clé publique  $(N, e)$ .

Un procédé de signature utilisant l'algorithme RSA consiste manière similaire à formater un message clair  $m$  par une fonction  $\mu'$  de formatage pour la signature, puis à réaliser une exponentiation du résultat selon la relation :

$$s = f^{-1}[\mu'(m)] = [\mu'(m)]^{d'} \bmod N'$$

où  $\mu'$  est une fonction de formatage pour la signature,  $(N', d')$  une clé privée, et  $f^{-1}(x, N', d')$  la fonction d'exponentiation  $f^{-1}(x, N', d') = x^{d'} \bmod N'$ .

La signature peut ensuite être vérifiée en utilisant à nouveau l'algorithme RSA, avec la fonction inverse  $f(x, N', e')$ ,  $(N', e')$  étant une clé publique associée à la clé privée  $(N', d')$ .

Les fonctions d'exponentiation et les fonctions de formatage (pour le chiffrement ou la signature) utilisées dans les systèmes cryptographiques sont en général connues. La sécurité des systèmes de cryptage dépend donc uniquement des clés privées et publiques utilisées. La clé privée doit être maintenue secrète.

La sécurité dépend ainsi notamment de la taille des clés, qui sont choisies de grande taille. Les nombres  $N$ ,  $N'$  sont généralement de grande taille, par exemple 1024 bits, ils sont égaux au produit de deux nombres premiers  $N = p \cdot q$ ,  $N' = p' \cdot q'$ . Les nombres  $d$ ,  $d'$  entiers dépendent des nombres  $N$ ,  $N'$  et sont également de grande taille. Les nombres  $e$ ,  $e'$  entiers sont par contre souvent de petite taille.

Pour des raisons de sécurité, les clés  $((N, e) ; (N, d))$  utilisées pour le chiffrement et les clés  $((N',$



$e')$  ;  $(N', d')$  utilisées pour la signature sont différentes.

Une fonction  $\mu'$  de formatage pour la signature est dite sûre s'il n'est pas possible de créer une signature  
 5 s d'un message  $m$  sans connaître la clé privée, même si un attaquant peut obtenir la signature d'autres messages de son choix. Les fonctions  $\mu'$  utilisées dans les systèmes cryptographiques sont construites pour vérifier cette condition.

10 Une fonction  $\mu'$  connue et sûre pour des opérations de signature est la fonction PSS (Probabilistic Signature Scheme, en français fonction probabiliste de signature), décrite notamment dans le document D1 (M. Bellare and P. Rogaway, The exact security of digital signatures- How to  
 15 sign with RSA and Rabin, Proceedings of Eurocrypt'96, LNCS vol 1070, Springer-Verlag, 1996, pp 399-416) et dans le standard PKCS#1 v2.1, RSA Cryptography Standard.

La fonction PSS est paramétrée par des entiers  $k, k_0, k_1$  et utilise deux fonctions de hachage :

$$\begin{aligned} 20 \quad H &: \{0, 1\}^{k-k_1} \rightarrow \{0, 1\}^{k_1} \\ G &: \{0, 1\}^{k_1} \rightarrow \{0, 1\}^{k-k_1} \end{aligned}$$

A partir d'un texte clair  $m$  de  $k - k_0 - k_1$  bits et d'un nombre  $r$  aléatoire de  $k_0$  bits, la fonction PSS produit :

$$25 \quad \text{PSS}(m, r) = \omega || s$$

avec  $r$  un paramètre aléatoire associé à la fonction PSS,  $||$  la fonction de concaténation,  $\omega = H(m || r)$ ,  $s = G(\omega) \oplus (m || r)$ , et  $\oplus$  la fonction logique XOR.

La signature  $s$  du message  $m$  est ensuite obtenue par  
 30 exponentiation à l'aide de la clé secrète  $(N, d)$  :

$$\begin{aligned} s &= f([ \text{PSS}(m, r) ], N, d) \\ &= [ \text{PSS}(m, r) ]^d \bmod N \end{aligned}$$

Une signature  $s$  peut être vérifiée en calculant :

$$35 \quad f^{-1}(s) = s^e \bmod N = \omega || s$$

où  $f^{-1}$  est la fonction inverse de la fonction d'exponentiation  $f$ .



Connaissant la taille de  $\omega$  et  $s$  (respectivement  $k_1$  bits et  $k-k_1$  bits), on déduit  $\omega$  et  $s$  de  $f^{-1}(s)$ . On calcule ensuite  $G(\omega) \oplus s$  à partir de  $\omega$ ,  $s$  et  $G$ . Comme  $G(\omega) \oplus s = M || r$ , on en déduit finalement  $H(m || r)$  et  
 5 m. Enfin, on compare  $\omega$  et  $H(m || r)$ . Si  $H(m || r) = \omega$ , alors le texte clair  $m$  est renvoyé, sinon seul un message d'erreur est renvoyé.

De manière similaire, une fonction  $\mu$  de formatage  
 10 pour le chiffrement est dite sûre s'il n'est pas possible, étant donnés deux messages clairs  $m_1$ ,  $m_2$ , de déterminer si un message chiffré  $c$  est le résultat du chiffrement du message  $m_1$  ou bien du message  $m_2$ . Cela doit rester impossible même si l'attaquant peut obtenir  
 15 le déchiffrement de n'importe quel message chiffré  $c'$  différent de  $c$ . Les fonctions  $\mu$  utilisées dans les systèmes cryptographiques sont construites pour vérifier cette condition de sécurité.

20 Cependant, parce que les critères de sécurité ne sont pas les mêmes pour des opérations de signature et des opérations de chiffrement, les fonctions  $\mu'$  de formatage pour la signature et les fonctions  $\mu$  de formatage pour le chiffrement ne sont pas les mêmes.

25 En conséquence, pour implémenter un système cryptographique complet, apte à chiffrer et déchiffrer, il est nécessaire de disposer de moyens pour mémoriser deux fonctions différentes, plus généralement deux algorithmes différents, et de disposer de moyens de  
 30 calcul programmés différents pour les mettre en œuvre. La taille du circuit électronique résultant est bien évidemment proportionnelle à la taille des algorithmes à mémoriser.

35 Pour résoudre le problème évoqué ci-dessus, selon l'invention, on utilise une même fonction de formatage, à



la fois comme fonction de formatage pour le chiffrement et comme fonction de formatage pour la signature. Plus précisément, selon l'invention, pour mettre en œuvre un procédé de chiffrement, on utilise la fonction PSS, connue par ailleurs pour mettre œuvre un procédé de signature.

Ainsi, l'invention concerne un procédé de chiffrement, comprenant une étape de formatage d'un message clair par une fonction de formatage, et une étape d'exponentiation du résultat de l'étape précédente à l'aide d'une clé publique selon la relation  $c = \mu(m)^e \bmod N$ ,  $c$  étant un message chiffré,  $\mu(m)$  étant le résultat de l'étape de formatage, et  $e$  et  $N$  des éléments de la clé publique.

Selon l'invention, la fonction de formatage est la fonction PSS.

La fonction PSS est une fonction sûre pour des opérations de chiffrement. En effet, on peut montrer que la fonction PSS est sûre pour des opérations de chiffrement, dans le modèle oracle aléatoire, tel que défini dans D2 : M. Bellare and P. Rogaway, Random oracles are practical : a paradigm for designing efficient protocols. Proceedings of the First Annual Conference on Computer Communication Security, ACM, 1993. Par ailleurs, actuellement dans le domaine de la cryptographie, la notion de sécurité dans le modèle oracle aléatoire est la notion de sécurité la plus forte pour des applications réelles.

Ainsi, selon l'invention, on dispose d'une fonction sûre à la fois pour des opérations de signature et des opérations de chiffrement.

L'invention concerne également un système de cryptographie comprenant un procédé de chiffrement et un procédé de signature, tous deux utilisant la fonction PSS comme fonction de formatage.



Plus précisément, le système cryptographique comprend :

- une étape de formatage d'un message clair par la fonction probabilistique de signature PSS, puis :

5        - si un chiffrement du message clair est souhaité, une étape d'exponentiation du résultat de l'étape de formatage à l'aide d'une première clé selon la relation  $c = \mu(m)^e \bmod N$ ,  $c$  étant un message chiffré,  $\mu(m)$  étant le résultat de l'étape de formatage, et  $e$  et  $N$  des éléments  
10 de la première clé, ou

      - si une signature du message clair est souhaitée, une étape d'exponentiation du résultat de l'étape de formatage à l'aide d'une deuxième clé ( $N'$ ,  $d'$ ) selon la relation  $s = \mu(m)^{d'} \bmod N'$ ,  $s$  étant un message signé,  $\mu(m)$   
15 étant le résultat de l'étape de formatage, et  $d'$  et  $N'$  des éléments de la deuxième clé.

Un tel système cryptographique est avantageux par rapport aux systèmes cryptographiques connus, dans la mesure où il nécessite environ deux fois moins de moyens  
20 (en termes de moyens de calcul programmés et de place mémoire notamment) pour être mis en œuvre.

Selon un mode de réalisation, la première clé et la deuxième clé sont respectivement une clé publique d'une première paire de clés et une clé privée d'une deuxième  
25 paire de clés.

Selon un autre mode de réalisation, préféré, la première paire de clé et la deuxième paire de clés sont identiques. En d'autres termes, le même jeu de clés est utilisé, à la fois pour mettre en œuvre le procédé de  
30 chiffrement et le procédé de signature. On montre en effet que déchiffrer un message, chiffré selon un procédé de chiffrement utilisant la fonction PSS et un jeu de clés donné, ne permet pas d'obtenir une information suffisante pour signer un message (éventuellement le  
35 message déchiffré) selon un procédé de signature utilisant la fonction PSS et le même jeu de clés. De



manière symétrique, on montre qu'obtenir une information sur la signature d'un message signé, selon un procédé de signature utilisant la fonction PSS et un jeu de clés donné, ne permet pas d'obtenir une information sur un message clair chiffré selon un procédé de chiffrement utilisant la même fonction PSS et le même jeu de clés.

L'invention est notamment applicable à l'algorithme de cryptographie RSA, qui est l'algorithme le plus utilisé à ce jour dans le domaine de la cryptographie.

L'invention concerne également un composant électronique comprenant des moyens programmés pour la mise en œuvre d'un procédé de chiffrement tel que décrit ci-dessus, utilisant la fonction PSS comme fonction de formatage. Les moyens programmés comprennent notamment une unité centrale et une mémoire de programme.

L'invention concerne encore un composant électronique comprenant des moyens programmés pour la mise en œuvre d'un système cryptographique tel que décrit ci-dessus, comprenant une opération de chiffrement ou une opération de signature, exécutées alternativement. Les moyens programmés comprennent notamment une unité centrale et une mémoire de programme.

L'invention est notamment intéressante pour des applications de type carte à puce, dans lesquels les composants utilisés doivent être de taille la plus petite possible, et la mise en œuvre des procédés la plus rapide possible.



## REVENDEICATIONS

1. Procédé de chiffrement, comprenant une étape de formatage d'un message clair (m) par une fonction de formatage ( $\mu$ ), et une étape d'exponentiation du résultat de l'étape précédente à l'aide d'une clé publique (N, e) selon la relation  $c = \mu(m)^e \bmod N$ , c étant un message chiffré,  $\mu(m)$  étant le résultat de l'étape de formatage, et e et N des éléments de la clé publique,

le procédé étant caractérisé en ce que la fonction de formatage ( $\mu$ ) est la fonction PSS.

10

2. Procédé selon la revendication 1, caractérisé en ce que la fonction de formatage  $\mu$  est définie par

$$\mu(m) = \text{PSS}(m) = \omega || s, \text{ avec :}$$

m, le texte clair de  $k = k_0 + k_1$  bits, r un paramètre aléatoire de  $k_0$  bits, k,  $k_0$ ,  $k_1$  étant des paramètres de la fonction de formatage,

$||$ , une fonction de concaténation

$$\omega = H(m || r)$$

$$s = G(\omega) \oplus (m || r),$$

20

$\oplus$  une fonction logique XOR, et

H, G deux fonctions de hachage

3. Utilisation d'une fonction probabilistique de signature (PSS) définie selon le standard PKCS#1 v2.1, RSA Cryptography Standard comme fonction de formatage ( $\mu$ ), pour réaliser un procédé de chiffrement comprenant une étape de formatage d'un message clair (m) par la fonction de formatage ( $\mu$ ), et une étape d'exponentiation du résultat de l'étape précédente à l'aide d'une clé publique (N, e) selon la relation  $c = \mu(m)^e \bmod N$ , c étant un message chiffré,  $\mu(m)$  étant le résultat de l'étape de formatage, et e et N des éléments de la clé publique.



4. Système cryptographique, comprenant :

- une étape de formatage d'un message clair (m) par la fonction probabilistique de signature (PSS), puis :

- si un chiffrement du message clair (m) est souhaité, une étape d'exponentiation du résultat de l'étape de formatage à l'aide d'une première clé (N, e) selon la relation  $c = \mu(m)^e \bmod N$ , c étant un message chiffré,  $\mu(m)$  étant le résultat de l'étape de formatage, et e et N des éléments de la première clé, ou
- si une signature du message clair (m) est souhaitée, une étape d'exponentiation du résultat de l'étape de formatage à l'aide d'une deuxième clé (N', d') selon la relation  $s = \mu(m)^{d'} \bmod N'$ , s étant un message signé,  $\mu(m)$  étant le résultat de l'étape de formatage, et d' et N' des éléments de la deuxième clé.

5. Système selon la revendication 3, dans lequel la première clé et la deuxième clé sont respectivement une clé publique d'une première paire de clés et une clé privée d'une deuxième paire de clés.

6. Système selon la revendication 4, dans lequel la première paire de clé et la deuxième paire de clés sont identiques.

7. Système selon l'une des revendications 4 à 6, de type RSA.

8. Composant électronique comprenant des moyens programmés pour la mise en œuvre d'un procédé de chiffrement selon l'une des revendications 1 à 2, les moyens programmés comprenant notamment une unité centrale et une mémoire de programme.

9. Composant électronique comprenant des moyens programmés pour la mise en œuvre d'un système



---

cryptographique selon l'une des revendications 4 à 7, les moyens programmés comprenant notamment une unité centrale et une mémoire de programme.

---

5      10. Carte à puce comprenant un composant électronique selon la revendication 7 ou la revendication 8.



DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 1. / 2.  
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

Vos références pour ce dossier (facultatif)		016596	
N° D'ENREGISTREMENT NATIONAL		020345	
TITRE DE L'INVENTION (200 caractères ou espaces maximum) Procédé de chiffrement de données, système cryptographique et composant associés.			
LE(S) DEMANDEUR(S) : GEMPLUS Avenue du Pic de Bertagne Parc d'Activités de GEMENOS 13420 GEMENOS			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		CORON	
Prénoms		Jean-Sébastien	
Adresse	Rue	domicilié au Cabinet BALLOT 9, rue Claude Chappe - Technopôle Metz 2000	
	Code postal et ville	57070	METZ
Société d'appartenance (facultatif)			
Nom		JOYE	
Prénoms		Marc	
Adresse	Rue	domicilié au Cabinet BALLOT 9, rue Claude Chappe - Technopôle Metz 2000	
	Code postal et ville	57070	METZ
Société d'appartenance (facultatif)			
Nom		NACCACHE	
Prénoms		David	
Adresse	Rue	domicilié au Cabinet BALLOT 9, rue Claude Chappe - Technopôle Metz 2000	
	Code postal et ville	57070	METZ
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire) Jean Louis LECLAIRE 93.4009			





# BREVET D'INVENTION

## CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



N° 11235\*02

### DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 2. / 2.

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

<b>Vos références pour ce dossier</b> (facultatif)		016596	
<b>N° D'ENREGISTREMENT NATIONAL</b>		0229475	
<b>TITRE DE L'INVENTION (200 caractères ou espaces maximum)</b> Procédé de chiffrement de données, système cryptographique et composant associés.			
<b>LE(S) DEMANDEUR(S) :</b> GEMPLUS Avenue du Pic de Bertagne Parc d'Activités de GEMENOS 13420 GEMENOS			
<b>DESIGNE(NT) EN TANT QU'INVENTEUR(S) :</b> (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
<b>Nom</b>		PAILLIER	
<b>Prénoms</b>		Pascal	
<b>Adresse</b>	<b>Rue</b>	domicilié au Cabinet BALLOT 9, rue Claude Chappe - Technopôle Metz 2000	
	<b>Code postal et ville</b>	57070	METZ
<b>Société d'appartenance (facultatif)</b>			
<b>Nom</b>			
<b>Prénoms</b>			
<b>Adresse</b>	<b>Rue</b>		
	<b>Code postal et ville</b>		
<b>Société d'appartenance (facultatif)</b>			
<b>Nom</b>			
<b>Prénoms</b>			
<b>Adresse</b>	<b>Rue</b>		
	<b>Code postal et ville</b>		
<b>Société d'appartenance (facultatif)</b>			
<b>DATE ET SIGNATURE(S)</b> <b>DU (DES) DEMANDEUR(S)</b> <b>OU DU MANDATAIRE</b> (Nom et qualité du signataire) Jean Louis LECLAIRE 93.4009			

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.  
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.



PCT Application  
**FR0302364**





**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☒ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**